FortiClient Rebranding Tool

The licensed FortiClient Rebranding Tool is used to create custom FortiClient installation files and rebrand FortiClient. Starting with FortiClient 5.6.0, a Site Toolkit subscription to Fortinet Developer Network (https://fndn.fortinet.net/) is required to access the licensed tool. Although you can use the tool in trial mode, a license key is required to access all of the features available with the tool.

The FortiClient Rebranding Tool is available for a Microsoft Windows operating system.

Overview

Following is an overview of using the FortiClient Rebranding Tool:

1. Prepare to download the subscription-based tool. See Prepare to download and license the tool on page 1.
2. Log into your FNDN account, add the activation code, and download the tool from FNDN. See Download the tool on page 2.
3. (Optional) Prepare configuration files and Telemetry gateway IP lists. See Prepare configuration files on page 2.
   You have the option to add a FortiClient configuration file and/or Telemetry gateway IP list to the FortiClient installer. Before you create the installer, you should get these files ready for selection.
4. Create a custom FortiClient installer. See Create custom FortiClient installation files on page 4.
   You will load the license key when you use the tool.
5. (Optional) Rebrand the FortiClient installer. See Rebrand FortiClient on page 10.
6. Deploy the custom FortiClient installation packages. See Deploy custom FortiClient installation packages on page 16.

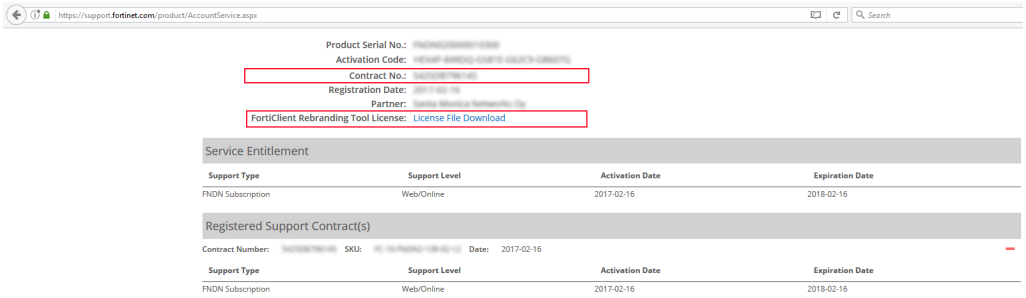
Prepare to download and license the tool

You must perform a number of tasks to access the FortiClient Rebranding Tool on FNDN.

To prepare to download and license the tool:

1. Purchase a Site Toolkit subscription to FNDN. Contact your Fortinet sales representative.
   A contract number for FNDN is generated. The contract number is included in the material that you receive for the purchase.
2. Register the contract number for FNDN with Fortinet Customer Service & Support at https://support.fortinet.com/.
   The registration process generates the following items:
   - Activation code for FNDN
   - License key file for FortiClient Rebranding Tool

You can retrieve the items from your account.



3. On the Fortinet Customer Service & Support site (https://support.fortinet.com/), go to *Asset* > *View Account Service* > *FNDN*, and download the license key from your account. You will add it to the FortiClient Rebranding Tool later.

   Place the license key in an easily accessible location. Because the FortiClient Rebranding Tool is not installed on the management computer, you must upload the license key each time that you run the tool to create a custom FortiClient installer. See Create custom FortiClient installation files on page 4.
4. Copy the activation code for FNDN. You will add it to your FNDN account later.

Download the tool

Download the licensed FortiClient Rebranding Tool from the Fortinet Developer Network site.

A Site Toolkit subscription to FNDN and an account to FNDN are required to access and download the FortiClient Rebranding Tool. See Prepare to download and license the tool on page 1.

To download the tool:

1. Log into your FNDN account at https://fndn.fortinet.net/.

   If you do not have an account for FNDN, you must create an account at https://fndn.fortinet.net/index.php?/register/.

   When you create an FNDN account, you are required to include the email address for two Fortinet sponsors. Fortinet sponsors are Fortinet employees who can verify that you are a Fortinet customer. Contact your sales representative or sales engineer for email addresses for Fortinet sponsors.
2. Add the activation code from your Fortinet Customer Service & Support at https://support.fortinet.com/ to your FNDN account settings.
3. Go to the *Tools* tab, and download the FortiClient Rebranding Tool.

Prepare configuration files

You can select the following types of files in the FortiClient Rebranding Tool when you create a custom FortiClient installer:

- Configuration file
- Gateway IP list

This section describes how to retrieve and edit the files to prepare them for use with the FortiClient Rebranding Tool.

You can use an XML editor to make changes to the FortiClient configuration file and Telemetry gateway IP list. For more information on FortiClient XML configuration, see the *FortiClient XML Reference* in the Fortinet Document Library at http://docs.fortinet.com.

Retrieve FortiClient configuration files

You can retrieve a configuration file from FortiClient console. The configuration file contains the settings for FortiClient. After you retrieve the configuration file, you can use an XML editor to make changes to the configuration file. Then you can select the FortiClient configuration file in the FortiClient Rebranding Tool.

To retrieve FortiClient configuration files:

1. In FortiClient console, go to *File* > *Settings*.
2. In the *System* area, click *Backup*.
3. Select a destination, and click *OK*.

Configure Telemetry gateway IP lists

You can retrieve a configuration file from FortiClient console to access the XML elements for the Telemetry gateway IP list.

If you are using FortiClient EMS (Enterprise Management Server), you can export a gateway IP list from FortiClient EMS. For details, see the *FortiClient 1.2 EMS Administration Guide*.

The Telemetry gateway IP list contains IP addresses for FortiGate and/or FortiClient EMS. FortiClient uses the Telemetry gateway IP list to connect FortiClient Telemetry to FortiGate or FortiClient EMS.

After you retrieve the configuration file, you can use an XML editor to locate the elements for the Telemetry gateway IP list and modify them.

To configure Telemetry gateway IP lists:

1. In FortiClient console, retrieve the configuration. See Retrieve FortiClient configuration files on page 3.
2. Open the configuration file in an XML editor.
3. Remove all elements, except the elements needed to configure the Telemetry gateway IP list. See Example XML of Telemetry gateway IP list on page 4.
4. Add IP addresses to the configuration file by using an XML editor.
   When using only FortiGate for endpoint control, use the `<fortigate>` element to identify one or more IP addresses for FortiGate devices.

When using FortiGate integrated with EMS, use the <fortigate> element to identify one or more IP addresses for FortiGate devices, and use the <notification_server> element to identify the IP address for EMS.

5. Save the configuration file.

Example XML of Telemetry gateway IP list

Following is an example XML file for a Telemetry gateway IP list. In this example, endpoints will connect Telemetry to FortiGate by using the IP addresses in the <fortigate> element and send notifications to FortiClient EMS by using the <notification_server> element.

```
<?xml version="1.0" encoding="UTF-8" ?>
   <forticlient_configuration>
      <endpoint_control>
         <enabled>1</enabled>
         <disable_unregister>0</disable_unregister>
         <silent_registration>1</silent_registration>
         <fortigates>
            <fortigate>
               <serial_number>fgt_sn0</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                     da7e6495841d8fc9c61067f81ef4cac01d697bb7e160c24d</registration_password>
               <addresses>172.30.254.150:8013</addresses>
            </fortigate>
            <fortigate>
               <serial_number>fgt_sn1</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                     6c9f088323beef31ea969c1c31c6db0e766273cb21851e68</registration_password>
               <addresses>172.30.254.174:8013</addresses>
            </fortigate>
            <fortigate>
               <serial_number>fgt_sn2</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                     7e819fa80a68ca2b602fdad54ba76190f03777c70399471d</registration_password>
               <addresses>172.30.254.158:8013</addresses>
            </fortigate>
            <notification_server>
               <address>us-ems1.myfortinet.com:8013</address>
            </notification_server>
         </fortigates>
      </endpoint_control>
   </forticlient_configuration>
```

Create custom FortiClient installation files

The following section provides instructions on creating a custom installer file using the FortiClient Rebranding Tool.

You have the option to select a FortiClient configuration file and/or Telemetry gateway IP list when you create a custom FortiClient installer. See Prepare configuration files on page 2.

Ensure that you select all modules in the FortiClient installer that you want installed on endpoints. To enable other features after FortiClient is installed, you must uninstall FortiClient from endpoints, and reinstall an MSI file with the desired features included in the FortiClient installer.

If you're using FortiClient EMS to deploy and manage FortiClient endpoints, you can create a FortiClient installer that includes most or all modules, and you can use a profile from FortiClient EMS to disable and enable modules without uninstalling and reinstalling FortiClient.

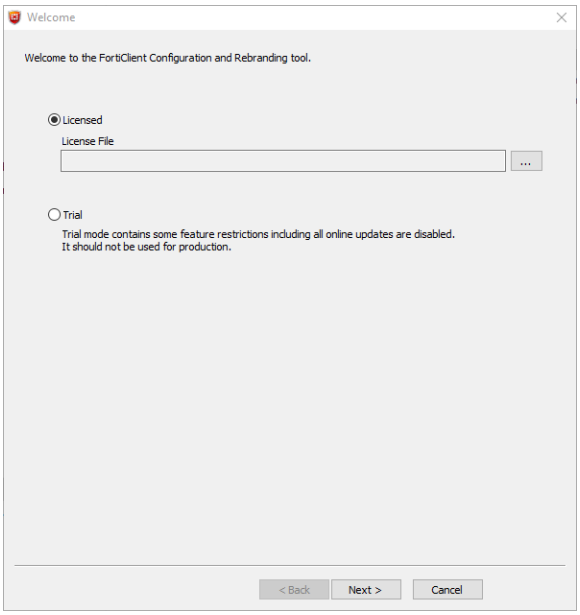
The FortiClient Rebranding Tool is not installed on the management computer. You must upload the license key file (.lic) each time you run the tool.

Use FortiClient Rebranding Tool for Windows

Windows has a hard limit of 260 characters on file path length. It is recommended to run the FortiClient Rebranding Tool in a shallow directory structure, such as c:\temp\, to avoid hitting the hard limit.

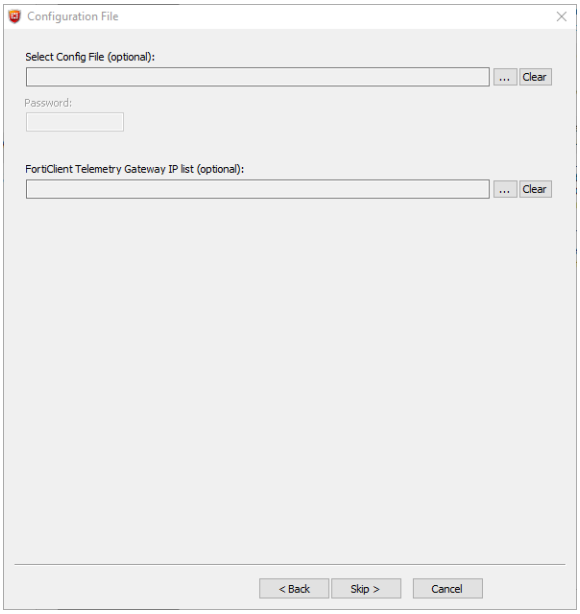
To create a custom FortiClient installation file:

1. Double-click the *FortiClientRebrandingTool.exe* application file to launch the tool.
   The *Welcome* page is displayed with the following options:



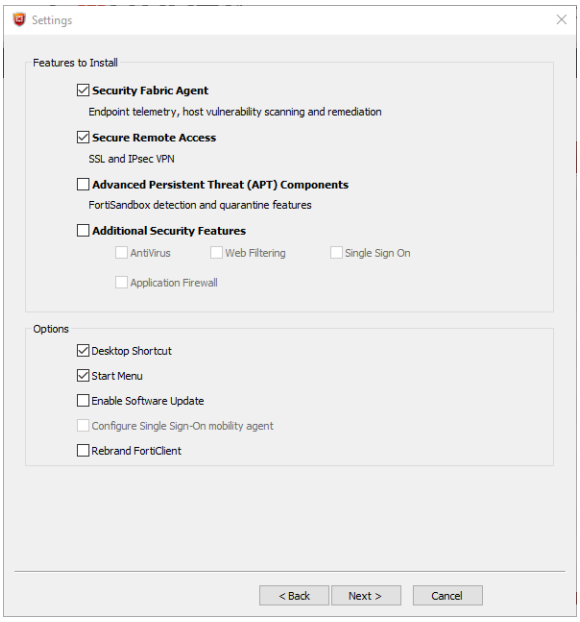
Licensed	Select to use the tool in licensed mode. Licensed mode requires a FortiClient Rebranding Tool license key. See also Prepare to download and license the tool on page 1.
Trial	Select to use the tool in trial mode. In trial mode, all online updates are disabled. The trial installer is intended to be deployed in a test environment.

2. Click the *Licensed* radio button, and click the *Browse* button.
3. Locate and select the license key, and click *Next*.
4. The *Configuration File* page is displayed with the following options.



Select Config File (optional)	Select a FortiClient configuration file (`.conf`, `.sconf`) to include in the installer file.
Password	If the FortiClient configuration file is encrypted (`.sconf`), enter the password used to encrypt the file.
FortiClient Telemetry Gateway IP List (optional)	Select a FortiClient Telemetry gateway IP list to include in the installer file. This option is disabled when using Trial mode.

Locate and select the FortiClient configuration file on your management computer, and click *Next*. If you do not want to include settings from a configuration file, click *Skip* to continue. The *Settings* page is displayed.

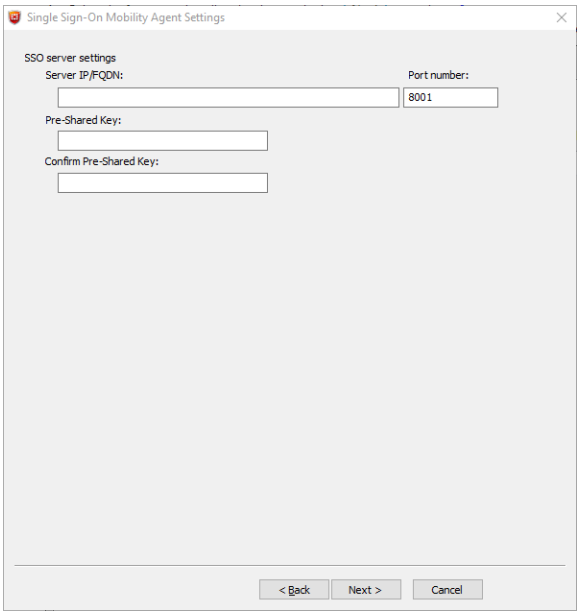


The following options are available for custom installations:

Features to Install	
Security Fabric Agent	Selected by default to support Fortinet Security Fabric. FortiClient Telemetry is always installed to support integration of FortiClient into the Security Fabric as follows: • Participate in compliance • Send user ID, avatar and email address to FortiGate • Be managed by EMS Along with the Vulnerability Scan component (also included in this agent), this provides the Security Fabric administrators an overview of the state of the endpoint. Clear the checkbox to exclude the *Compliance* tab and *Vulnerability Scan* tab from the FortiClient installation file.
Secure Remote Access	Select to include SSL and IPsec VPN modules in the FortiClient installation file.
Advanced Persistent Threat (APT) Components	Select to include FortiSandbox detection and quarantine modules in the FortiClient installation file.
Additional Security Features	Select to include one or more of the following modules in the FortiClient installation file: • AntiVirus • Web Filtering • Single Sign On • Application Firewall

Options		
	Desktop Shortcut	Select to create a FortiClient desktop icon on the endpoint.
	Start Menu	Select to add FortiClient to the start menu on the endpoint.
	Enable Software Update	Select to enable FortiClient software updates via FortiGuard Distribution Network on endpoints. This option is disabled when *Rebrand FortiClient* is selected. This option is also disabled when using trial mode.
	Configure Single Sign-On mobility agent	Select to configure Singe Sign-On mobility agent for use with FortiAuthenticator. You must select the *Single Sign On* checkbox in the Features to Install area first.
	Rebrand FortiClient	Select to rebrand FortiClient. When selected, the option to enable software update is not available.

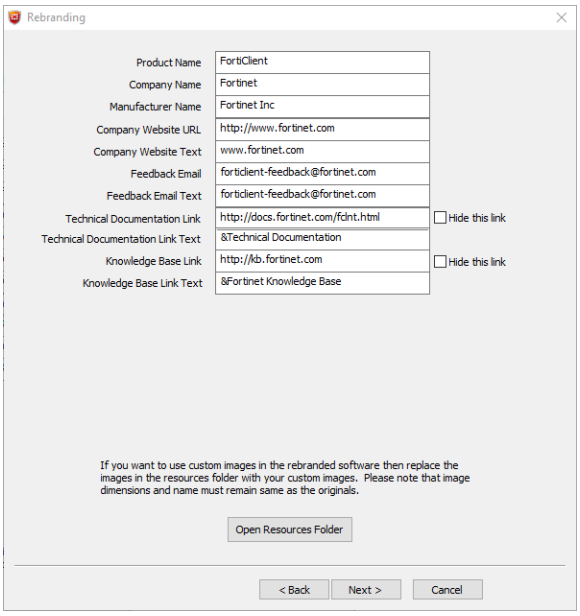
5. Select the features to install and options, and click *Next* to continue.
   If you selected the *Configure the single sign-on mobility agent* check box, the *Single Sign-On Mobility Agent Settings* page is displayed.



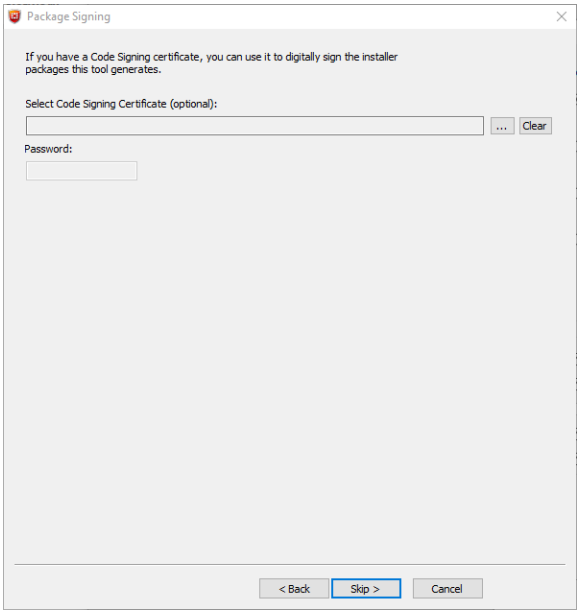
6. Configure the following settings:

Server IP/FQDN	Enter the IP address or FQDN of the FortiAuthenticator server.
Port number	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the FortiAuthenticator pre-shared key.
Confirm Pre-Shared Key	Enter the FortiAuthenticator pre-shared key confirmation.

7. Select *Next* to continue.
   If you selected to rebrand FortiClient, the *Rebranding* page is displayed.



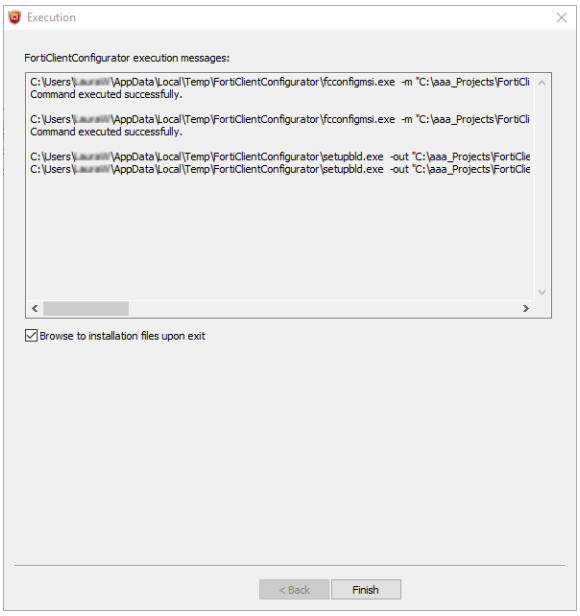
8. Rebrand FortiClient elements as required. The resources folder contains graphical elements.
9. Click *Next* to continue. The *Package Signing* page is displayed.



10. Configure the following settings:

Select Code Signing Certificate (optional)	If you have a code signing certificate, you can use it to digitally sign the installer package this tool generates.
Password	If the certificate file is password protected, enter the password.

11. (Optional) Browse and select the code signing certificate on your management computer. If you do not want to digitally sign the installer package, select *Skip* to continue. The *Execution* page is displayed.



This page provides details of the installer file creation and the location of files for Active Directory deployment and manual distribution. The tool creates files for both 32-bit (x86) and 64-bit (x64) operating systems.

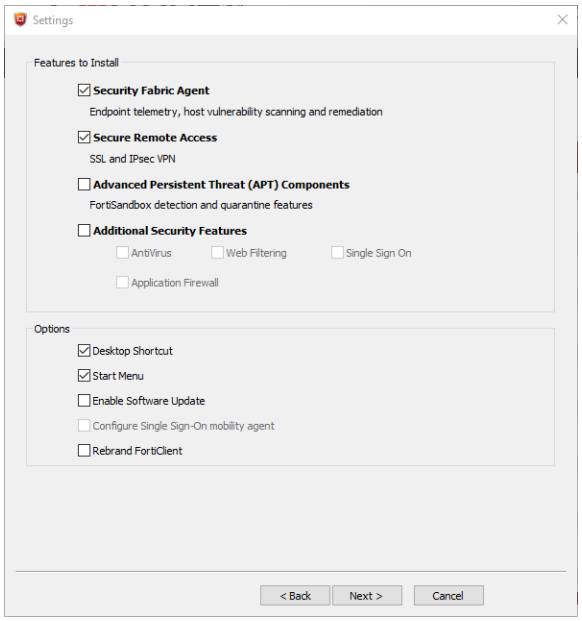
12. When you click *Finish*, the folder containing the newly created MSI file will open when the *Browse to installation files upon exit* checkbox is selected.

Before deploying the custom MSI files, it is recommended that you test the packages to confirm that they install correctly. An `.exe` installation file is created for manual distribution.

Installation files are organized in folders within the folder where you placed the *.exe* file for the FortiClient Rebranding Tool. Folder names identify the type of installation files that were created and the creation date.

Rebrand FortiClient

The FortiClient Rebranding Tool can be used to create custom FortiClient MSI installers with various combinations. The customized MSI installer generated may be used to install FortiClient on all supported platforms using Active Directory. A FortiClient setup executable file is also generated for manual distribution.



Under *Options*, you can select to enable software updates, configure the single sign-on mobility agent, and rebrand FortiClient. Rebranding allows you to edit various UI elements including graphics.

When replacing files in the resource folder, the replacement file should be the same file type and dimensions. Icons (`.ico`) are a special case. The `Main_icon.ico` file for example, is a composite file of multiple icons. The operating system picks the appropriate icon size from this file for the context in which the icon is being displayed.

Rebranding elements:

Installer Product Name	Where Used: Setup Wizard header and body, File directory name in Installer Company Name file folder, engine/signature update bubble messages. Default Value: FortiClient
Installer Company Name	Where Used: File directory name in Program Files. Default Value: Fortinet
Manufacturer Name	Where Used: Default Value: Fortinet Inc
Company WebSite URL	Where Used: *Help* > *About* > *Copyright* page Default Value: http://www.fortinet.com
Company Website Text	Where Used: *Help* > *About* > *Copyright* page Default Value: www.fortinet.com
Feedback Email	Where Used: *Help* > *About* > *Copyright* page, Send Feedback Default Value: forticlient-feedback@fortinet.com
Feedback Email Text	Where Used: *Help* > *About* > *Copyright* page, Send Feedback Default Value: forticlient-feedback@fortinet.com

Knowledge Base Link	Where used: Link used by Knowledge Base text Default value: http://kb.fortinet.com Leave this field blank to omit the field in the console.
Knowledge Base Link Text	Where Used: Help menu option Default Value: Fortinet Knowledge Base Leave this field blank to omit the field in the console.

Resources folder elements:

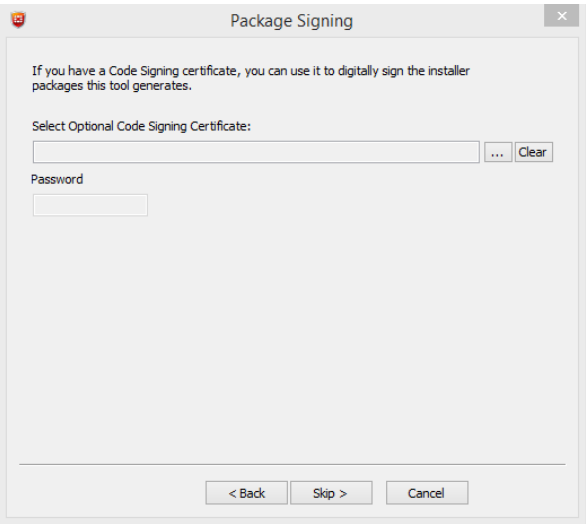
About_red_shield_logo.png	Where Used: File Type: PNG File (.png) Width: 43 pixels Height: 43 pixels Bit Depth: 32
Advertisement_ad_0.png	Where Used: Dashboard advertisement banner File Type: PNG File (.png) Width: 628 pixels Height: 66 pixels Bit Depth: 32
Advertisement_ad_1.png	Where Used: Dashboard advertisement banner File Type: PNG File (.png) Width: 628 pixels Height: 66 pixels BitBit Depth: 32
Advertisement_ad_2.png	Where Used: Dashboard advertisement banner File Type: PNG File (.png) Width: 628 pixels Height: 66 pixels Bit Depth: 32
Antivirus_AV_scan_top_banner_left_hand_side.png	Where Used: File Type: BMP File (.bmp) Width: 1 pixel Height: 40 pixels Bit Depth: 8
Antivirus_AV_scan_top_banner_right_hand_ side.png	Where Used: Banner used in right-click “scan with product name” dialog box File Type: BMP File (.bmp) Width: 440 pixels Height: 40 pixels Bit Depth: 8

Common_fgt-not-found-page-bg.png	Where Used: FortiGate not found page File Type: PNG File (.png) Width: 673 pixels Height: 189 pixels Bit Depth: 32
Common_fortinet-icon.png	Where Used: File Type: PNG File (.png) Width: 79 pixels Height: 79 pixels Bit Depth: 32
Common_registration_icon.png	Where Used: FortiGate detected page File Type: PNG File (.png) Width: 85 pixels Height: 85 pixels Bit Depth: 32
Common_searching-page-bg.png	Where Used: Searching for FortiGate page File Type: PNG File (.png) Width: 673 pixels Height: 189 pixels Bit Depth: 32
Dashboard_forticlient_v5_dashboard_bg.png	Where Used: Client console File Type: PNG File (.png) Width: 628 pixels Height: 451 pixels Bit Depth: 32
Dashboard_warning-shield.png	Where Used: Dashboard warning shield, displayed when antivirus is disabled. File Type: PNG File (.png) Width: 59 pixels Height: 75 pixels Bit Depth: 32
Installer_background.bmp	Where used: Setup Wizard background image. File Type: BMP file (.bmp) Width: 491 pixels Height: 312 pixels Bit Depth: 8

Installer_banner.bmp	Where Used: Setup Wizard banner image on destination page, ready to install page, installing pages. File Type: BMP file (.bmp) Width: 491 pixels Height: 58 pixels Bit Depth: 8
LightInstaller_icon.ico	Where Used: Light Installer Icon File Type: ICO File (.ico) Width: 32 pixels Height: 32 pixels Bit Depth: 32
Main_icon.ico	Where Used: Shortcut on desktop File Type: ICO file (.ico) Width: 48 pixels Height: 48 pixels Bit Depth: 32
Main_logo_black.ico	Where Used: Client console header File Type: ICO file (.ico) Width: 32 pixels Height: 32 pixels Bit Depth: 32
setup.ico	Where Used: Setup icon File Type: ICO File (.ico) Width: 256 pixels Height: 256 pixels Bit Depth: 32
Tray_Icons_alert.ico	Where Used: System tray alert icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_alert_vpn.ico	Where Used: System tray VPN alert icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32

Tray_Icons_running.ico	Where Used: System tray running icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_scan1.ico, Tray_Icons_scan2.ico, Tray_Icons_scan3.ico, Tray_Icons_scan4.ico, Tray_Icons_scan5.ico, Tray_Icons_scan6.ico, Tray_Icons_scan7.ico, Tray_Icons_scan8.ico, Tray_Icons_scan9.ico, Tray_Icons_scan10.ico Tray_Icons_scan11.ico	Where Used: System tray, these eleven images animate the scanning activity of the tray icon. File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_vpn.ico	Where Used: System tray VPN icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
VPN_xauth-dialog-logo.png	Where Used: VPN xAuth dialog logo File Type: PNG File (.png) Width: 88 pixels Height: 100 pixels Bit Depth: 32
zzz_rebranding.ini	Where Used: This file is used by the FortiClient Configurator tool for element/resource mapping. File Type: Configuration settings (.ini)

When rebranding FortiClient, you can select to digitally sign the installer package using a code signing certificate.



Deploy custom FortiClient installation packages

After the FortiClient Rebranding Tool generates the custom installation packages, you can use the custom installation packages to deploy FortiClient (Windows) software either manually, or using Active Directory. Both options can be found in the *.../FortiClient_packaged* directory. Files are created for both x86 (32-bit) and x64 (64-bit) operating systems.

If you are using Active Directory to deploy FortiClient (Windows), you can use the custom installer with the MST file found in the *.../ActiveDirectory* folder.

For manual distribution, use the `.exe` file in the *.../ManualDistribution* folder.